Healthcare Cybersecurity Perspectives from the Michigan Healthcare Cybersecurity Council

Presented by Doug Copley, Chairman – Michigan Healthcare Cybersecurity Council

Mr. Chairman and Committee Members,

I'd like to thank you for allowing me the opportunity to provide cybersecurity perspectives in healthcare to the Senate Energy & Technology Committee this afternoon. My name is Doug Copley. I am an IT Director and Information Security Officer for Beaumont Health System, a $2.2 billion dollar, nearly 1,800 bed health system located in metropolitan Detroit. I am also the Chairman of the Michigan Healthcare Cybersecurity Council, comprised of 29 institutions across the state of Michigan. The Michigan Healthcare Cybersecurity Council (MHCC) was established to protect the critical healthcare infrastructure in the State of Michigan from cybersecurity threats, and to mature and advance the state of cybersecurity preparedness across the healthcare industry in Michigan.

The challenges facing the healthcare industry are significant. Hospitals, clinics, and health plans are faced with the challenge of improving patient outcomes, maintaining quality, providing more convenient and personal care, allowing patients to track their own health, allowing providers seamless access to patient data regardless of their location or device, and working with health information exchanges to provide data across organizations. Meanwhile, healthcare organizations must make sure all the data is appropriately controlled and safeguarded from the ever-increasing range of threats, including cyber threats – all while reducing costs. Understanding that large electronic medical record (EMR) systems alone can be multi-million dollar ANNUAL investments, for many of the non-profit healthcare organizations across the state, meeting all these challenges concurrently is an unrealistic expectation without support from outside their organization.

Threats and Concerns in Healthcare:

Threats to organizations and to patient data continue to challenge healthcare entities. Some 94% of healthcare organizations have reported at least one HIPAA breach, according to a 2012 study from the Ponemon Institute. Unfortunately, 52% of those breaches were found during an audit or an assessment.

Another study of the healthcare industry showed that in 77% of cases, the average time from initial attack to compromise of data was measured in minutes, while in 78% of cases, the time from initial compromise to discovery of the compromise was measured in weeks and months. This statistic demonstrates the significantly less mature ability within healthcare to detect and respond to attacks in a timely manner.

There are various risks in healthcare, which can threaten organizations and patients in different ways. Some of those include:

- Patient identity theft and credit card fraud
- Medical insurance fraud (charging insurance companies for fraudulent procedures)
- Medical insurance fraud (getting medical treatment using someone else's information)
- Medical device hacking (to obtain data or cause personal harm to someone)

For identity theft and fraud to occur, patient data is being removed from organizations via malicious insiders, mistakes, hacking via poor safeguards, social engineering of staff or patients themselves, or many other avenues.

Recent Breaches:

- University of Washington Medicine has 90,000 records exposed when an employee clicked on an email attachment with malware. **Solution**: education
- Sep'13: Advocate Health exposed 4,000,000 patient records when 4 unencrypted laptops were stolen. **Solution**: encrypt mobile devices
- Oct'13: AHMC exposed 729,000 records when 2 unencrypted laptops were stolen. **Solution**: encrypt
- Oregon Health & Science University exposed 3,000 patient records when residents and physicians were using Google Drive and Gmail to store and transmit patient protected health information. **Solution**: education and technology alternatives
- Medical University of South Carolina exposed 7,000 records when hackers attacked their online credit card payment systems **Solution**: secure systems better
- Dick Cheney had the wireless capability in his pacemaker removed for fear that malicious individuals would be able to hack the device and potentially stop his heart.

Some of the most common reasons data breaches occur are the following:

- Poorly educated staff
- 3rd parties that don't adequately protect the data
- Insider privacy breach (1-off)
- Malicious insider data theft
- Unsecured devices holding patient data
- Hacking medical equipment or systems providing online access to patient records
- Malware spread through non-company devices

Direction from the Federal Government

As you are aware, healthcare is one of 18 federally-identified critical infrastructures. 90% of those critical infrastructure sectors are owned or operated by non-government entities.

From a federal government perspective in regards to cybersecurity, **Executive Order 13636: Improving Critical Infrastructure Cybersecurity** directs the Executive Branch to:

1. Develop a technology-neutral voluntary cybersecurity framework
2. Promote and incentivize the adoption of cybersecurity practices
3. Increase the volume, timeliness and quality of cyber threat information sharing
4. Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
5. Explore the use of existing regulation to promote cyber security

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:

1. Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
2. Understand the cascading consequences of infrastructure failures
3. Evaluate and mature the public-private partnership
4. Update the National Infrastructure Protection Plan

5. Develop comprehensive research and development plan

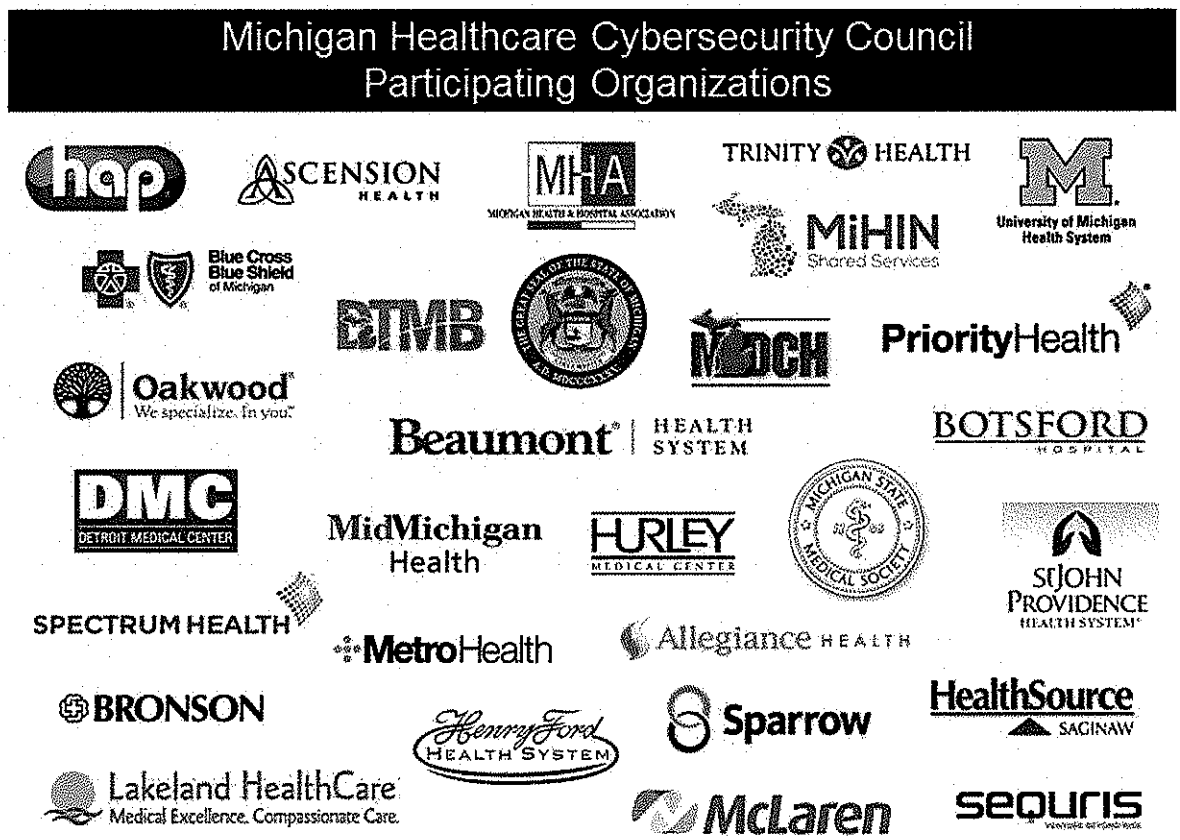
Michigan Healthcare Cybersecurity Council

In June 2013, in support of the **Michigan Cyber Initiative** and through the leadership of David Behen, State of Michigan CIO, Dan Lohrmann, State of Michigan CSO, Subra Sripada , Beaumont Health System CIO, and Doug Copley, Beaumont Health System ISO, the Michigan Healthcare Cybersecurity Council was formed. The MHCC is an independent, public-private partnership in the State of Michigan involving hospitals and healthcare systems, payer organizations, physician organizations and supporting members such as the Michigan Department of Technology, Management and Budget, The Michigan Department of Community Health, the Michigan Health and Hospital Association and the Michigan Health Information Network. The mission of the MHCC is to protect the critical healthcare infrastructure in the State of Michigan from cybersecurity threats, and to mature and advance the state of cybersecurity preparedness across the healthcare industry in Michigan. Three members of the Council are also members of the State of Michigan CSO Kitchen Cabinet and have contributed to the State of Michigan Cyber Disruption Response Strategy.

In support of its mission, the objectives of the MHCC include:

- Assessing cybersecurity risks that are most significant to the state's healthcare infrastructure
- Developing solutions to common challenges and delivering actionable work product that can be consistently applied across the healthcare industry in Michigan
- Recommending and reviewing appropriate legislation to support healthcare cybersecurity efforts in the State
- Providing a forum and protocols for State and industry security leaders to engage each other for advice and/or assistance
- Advocating with other interdependent organizations to support the MHCC mission
- Informing industry stakeholders of progress and outcomes they may be able to apply within their own organizations

In its first seven months, the MHCC has conducted five productive meetings, participated in the 2013 Michigan Cyber Summit, established three priority initiatives and convened sub-committees for each. The three priority initiatives are medical device security, a security framework for Michigan healthcare organizations, and incident response. Our Council is committed to exhibiting meaningful progress in these key areas in 2014. The Council determined these areas to be the highest priority, and areas with the most potential to benefit all healthcare organizations across the state and improve the overall posture and maturity of cybersecurity preparedness across the industry in Michigan. The Council meetings rotate locations among the participating organizations. The most recent meeting of the Council was Thursday, January 16th at CHE/Trinity Health in Livonia.



Conflicting Priorities for Health Systems

When it comes to cybersecurity preparedness, healthcare providers have conflicting priorities to reconcile. Because most health systems in Michigan are non-profit and operate at very low operating margins, prioritization of capital and operational spending is critical, and often patient care efforts are prioritized above cybersecurity initiatives because they directly support the organizational or community mission. In addition, Medicare and Medicaid reimbursements continue to decline, thus putting cybersecurity initiatives at even higher risk of not being funded. Stated very simply, healthcare institutions do not have the resources of other industries such as financial services, to address cybersecurity adequately.

Electronic medical records, meaningful use initiatives, health information exchanges and the push for accountable care add even further conflict to the prioritization of cybersecurity initiatives. The push to make patient medical records and results available at the point of need to internal providers, external providers and even patients themselves increases the need to ensure the secure transmission and remote access to medical records are safe, secure and cannot be exploited by cybersecurity threats. Thus the need to enhance cybersecurity preparedness has increased at the same time the funding continues to be at-risk. As a former security manager and privacy executive in financial services, I can convey that the state of cybersecurity preparedness in healthcare lags significantly behind the capability of more mature industries such as financial services, manufacturing and energy.

To summarize,

- Our purpose as a healthcare provider is to provide effective patient care
- Most hospitals in Michigan are non-profit and operate at very low margins (1-2%)
- Medicare and Medicaid continue to decrease reimbursements for medical treatment
- Funding is needed to incorporate sufficient security measures in healthcare, and to protect systems from cybersecurity threats

- Providers are being pushed by current legislation to share patient data faster, easier with more providers and exchanges (which enhances the need for more mature security capabilities) (Affordable Care Act and Meaningful Use initiatives)
- Every dollar spent on the security program is 1 less dollar spent on patient care, doctors, nurses, etc. which goes against company missions

Priorities for Council Funding:

During prior Council meetings, strategic priorities and future opportunities for the Council were discussed. To affect the most positive change across healthcare in Michigan while supporting national efforts in cybersecurity preparedness, the following initiatives were identified and determined to require external funding:

- Establish permanent staff to manage the day-to-day operations and coordinate sub-committee activities of the Council. The executives involved in the Council are limited in their ability to commit time outside of the meetings, so a limited amount of permanent resources would help progress the initiatives of the Council at a faster pace. Approximately $900,000 would be needed to support the first 2 years of the Council's activities. After 2 years, a sustaining funding model would need to be established (see items below).

- Establish a certification capability for the Council (if established as a non-profit legal entity), similar to the Texas Health Services Authority, to certify:
    - Michigan healthcare institutions against a set of commonly-established criteria (cybersecurity framework) such as those provided by HiTrust and NIST (and make those available to the State of Michigan and organizations participating in the Council). This can be used to measure maturity levels in healthcare cybersecurity preparedness across Michigan.
    - To certify 3rd party healthcare providers to do business in the State, especially those qualifying as Business Associates, (at their expense) against common criteria and make those certifications and analysis available to Michigan healthcare organizations as evidence of due diligence in the areas of security and privacy. This benefits not only the healthcare organizations, but also alleviates the need for 3rd party providers to complete multiple security/privacy assessments from multiple healthcare companies. (Texas has already taken this step)
    - Qualified HIE applicants within the state of Michigan to ensure they are operating under accepted and uniform standards in the handling of protected health information. (This activity may fall within the mission and scope of the Michigan Health Information Network today)

  A more formal analysis of the amount of funding required to establish this capability needs to be completed, but we anticipate that approximately 2-3 million dollars would be necessary to establish the processes and complete assessments of State healthcare institutions. Assessments of 3rd-party providers would be funded by the provider. This may also require legislation allowing the Council to be the authority for the certifications.

- Establish a Michigan Healthcare Information Sharing and Analysis Center (ISAC) which would provide common, shared capabilities in the following areas:
    - Threat monitoring
    - Vulnerability monitoring
    - Incident response

  This would require several million dollars to establish (for licensing tools and establishing connectivity and processes to manage it) and a future funding model supported by the participating organizations would need to be established. A specific funding analysis has not been completed at this time.

Legislative Perspectives and Necessary Assistance

One key success established with the Michigan Healthcare Cybersecurity Council is the willingness and ability to share information and make progress toward industry-wide cybersecurity preparedness without additional laws or regulations. In considering future potential initiatives for the Council, additional legislation may be needed, and is outlined below:

1. Legislate or advocate for streamlined processes to make it easier for non-public security leaders in critical infrastructure sectors to obtain secret government security clearance. Executive Order 13636 item 3 and PPD-21 item 3 support this at a federal level, but the processes to foster that sharing are not in place and it's a very difficult process for individuals from non-public entities to obtain secret clearance. This item was discussed at the last State of Michigan CSO Kitchen Cabinet Meeting and it was determined that governmental processes needed to be streamlined between the Michigan State Police and the Department of Defense or Department of Homeland Security to address this area.

2. Put legislation in place to allow the Council (if established as a non-profit legal entity) to be the certification authority for those items identified in the Priorities for Council Funding section above.

Mr. Chairman and committee members, I hope you found these perspectives on cybersecurity challenges in healthcare valuable and I thank you once again for allowing me to present this important information to you today.